

Graphical models of Separation Logic

Tony Hoare

Concurrency Theory Workshop

14 Jan 2009

Goal: Unification

- of memory with communication
- of strong memory consistency with weakness of various kinds
- of synchronised, two-ended communication with buffering, multiplexing, re-ordering, stuttering, loss, forgery,...
- maintain validity of rely-guarantee reasoning

Summary

- It's impossible
- It's trivial
- It's a cheat

Semantics

- A program P is a set of traces
- A trace p is a set of events
 - with a dependency relation \rightarrow
 - representing flow of data, control, or ownership
 - with transitive closure \rightarrow^*
- $P * Q = \{p + q \mid p \in P \ \& \ q \in Q\}$
 - each event is attributed to one of P or Q
- Theorem: $*$ is a Kleene composition

Weak sequence

- $P ; Q = \{ p + q \mid p \in P \ \& \ q \in Q \ \& \ \neg \exists e, f . e \in P \ \& \ f \in Q \ \& \ f \rightarrow^* e \}$
 - allows re-ordering optimisations
 - and weak memory models
 - in combination!
- Theorem: $;$ is a Kleene composition

Theorems

- Exchange law
- Corollaries

Theorem

- distribution law

Rely-guarantee

- $P \text{ R } \{C\} \text{ G } S \quad = \quad P ; (R^*C) \subseteq S \ \& \ C \subseteq G$
- Theorem: all the laws of rely-guarantee are valid.